Government Mobile and Wireless Security Baseline

May 23, 2013

Table of Contents

Table of Figures

Table of Tables

Executive Summary

The Digital Government Strategy (DGS),[1] issued by the Federal Chief Information Officer (CIO) in May 2012, describes a vision that applies the power and innovation of digital technology to enable citizens and an increasingly mobile workforce to securely access digital information and services anywhere, anytime, and on any device. The strategy recognizes the challenges of integrating effective security and privacy in mobile devices, applications, and wireless networks.

To promote the safe and secure adoption of new technologies, DGS milestone action 9.1 tasked the Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST) with developing a baseline of standard security requirements for mobile computing, and a Mobile Security Reference Architecture (hereafter "Reference Architecture") that incorporates security and privacy by design. Experts from NIST, DHS, DoD, the Department of Justice, the General Services Administration (GSA) and other members of the Mobile Technology Tiger Team (MTTT) formed a technical working group to develop the mobile security baseline. The Reference Architecture was also developed as a cooperative interagency effort led by DHS Federal Network Resilience Division.

This document contains the mobile security baseline and explains its relationship to the Reference Architecture, the Mobile Computing Decision Framework, and other DGS mobile security activities. It builds on the DGS report for milestone action 10.2, Government Use of Mobile Technology: Barriers, Opportunities and Gap Analysis (hereafter "DGS Barriers and Opportunities report"), which identifies four key areas that require improvements in tools and processes to "accelerate the secure adoption of mobile technologies into the Federal environment":

1) Mobile Device Management (MDM);
2) Mobile Application Management (MAM);
3) Identity and Access Management (IAM); and
4) Data Management.

The DGS Barriers and Opportunities report described a set of typical use cases for digital government services (public, partners, state-local-tribal-territorial, Federal employee, and national security systems). To develop the mobile security baseline, the use cases were separated into agency controlled and non-agency controlled device scenarios, and overlaid with the four key elements for secure mobile computing, indicating the need to address these four functions for each use case. For each use case, the Federal Mobility Use Cases section explains the user population, interactions with Government agencies, the type

[1] Digital Government: Building a 21st Century Platform to Better Serve the American People (May 23, 2012), http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf.

of applications, services and information to be accessed from mobile devices, and the location of the user and the information. The mobile security baseline, which follows NIST standards and guidelines, is focused on the Federal employee use case.

To set the context for the Mobile Security Baseline and the Reference Architecture, the first section of this document explains the essential elements of mobile computing (devices, access networks, agency infrastructure), and describes threats and risks to mobile computing. This document includes an overview of the Reference Architecture and the Mobile Computing Decision Framework (MCDF) published by DHS Federal Network Resilience (FNR). It provides guidance on how to use the MCDF to help Departments/Agencies (D/As) define their requirements and risk tolerance, select D/A's mobile security architecture and apply the security controls defined in the mobile security baseline.

Appendix A, Federal Mobile Computing Security Baseline, contains the moderate baseline for the most common Federal mobility use case: *Federal employees operating agency-controlled mobile devices to access moderate impact systems on a Federal network.* It includes the core controls for MDM and MAM, and notional controls for IAM and data management. Appendix B describes Technical Exchange Meetings (TEM) conducted to socialize the use cases and mobile security baseline with government and industry.

This document provides guidance to aid D/As in implementing secure mobile solutions as part of their information security program. Nothing in this document is intended to replace or supersede mandatory Federal and D/A requirements regarding protection of Federal information and information systems.

Mobile Computing Overview

Mobile computing technology allows Federal D/As to address demand from the workforce and citizens for access to government information and services unrestricted by user location or time of day. Mobile computing extends from mobile devices, through wireless and wired access networks, to the D/A systems and infrastructure that provide digital government services. The mobile computing environment encompasses the following elements.

Mobile Devices

Mobile devices include smartphones and tablet computers that support multiple wireless network connectivity options (primarily cellular and Wi-Fi), and host voice and data applications. The devices run mobile operating systems which are used to access mobile sensors, data and voice services.

Access Networks

Access networks include commercial cellular providers and Wi-Fi networks. These networks provide wireless network access to mobile device users that allow them to connect to the Internet and to D/A enterprise services. Mobile devices are designed to natively take advantage of any wireless network connectivity available. These wireless networks may be trusted (secure enterprise wireless network), untrusted (public Wi-Fi), or hostile (foreign telecom provider's network).

Enterprise Infrastructure

Enterprise infrastructure encompasses mobility access gateways and management services and D/A information and services. Mobility infrastructure provides the enterprise connection for communications with mobile devices, and the systems/services to manage devices, applications and authentication. The D/A's enterprise services are the existing and evolving services provided for all enterprise users, including mobile users. These services include voice and data communications (e.g., email, chat, or calendar), as well as productivity, collaboration, and mission-related applications and services.

Figure 1: Generic Mobile Computing Architecture depicts the devices, access networks, and enterprise infrastructure that comprise mobile computing architecture. The figure includes the four key areas identified in the DGS Barriers and Opportunities report developed for Milestone Action 10.2:

1) Mobile Device Management (MDM);
2) Mobile Application Management (MAM);
3) Identity and Access Management (IAM) solutions for use with mobile devices; and
4) Data Management, including authentication and encryption solutions that meet Federal requirements.

Since smartphones and tablets are primarily consumer devices, additional tools are required to support corporate/government use. Improvements are needed in the available tools and processes that provide these management functions for secure D/A enterprise mobility management. To provide context for the description of security functions provided by each of these areas, the following section explains common threats and risks to mobile computing.

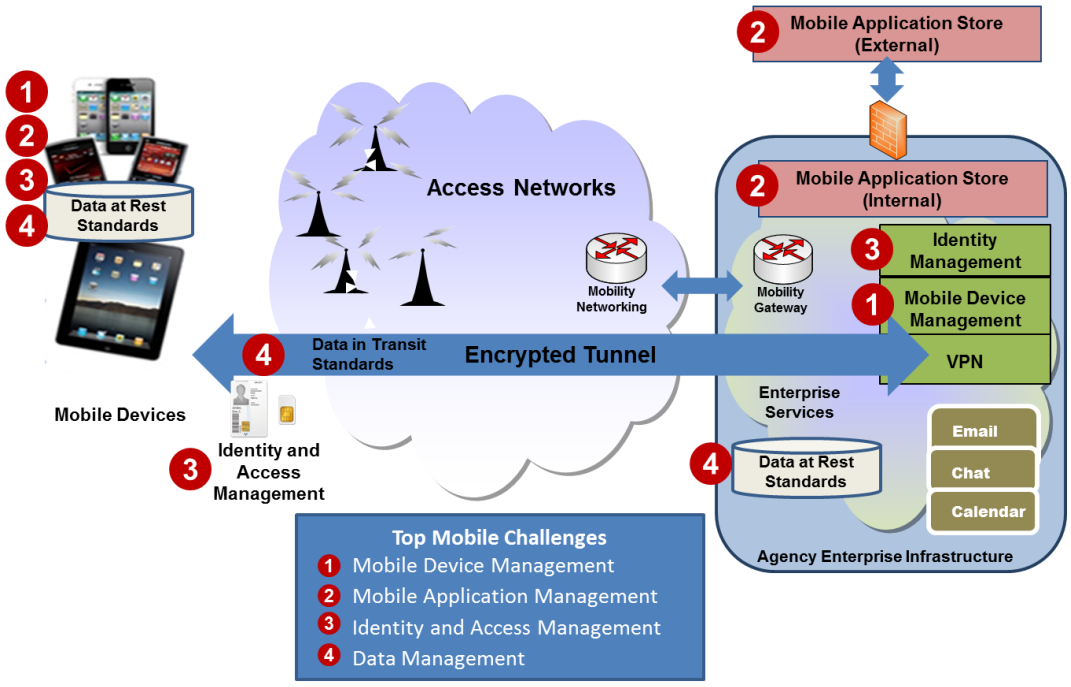


Figure 1: Generic Mobile Computing Architecture

Understanding Mobile Threats, Risks and Mitigations

Mobile devices face some of the same threats as desktop computers. However, these devices are subject to additional unique threats because of their size, portability, always-on wireless connections, physical sensors (e.g., camera, microphone) and location services (e.g., Global Positioning System). The diversity of available devices, operating systems, carrier-provided services (e.g., Short Message Service, browser, e-mail), and mobile applications present additional security challenges to the confidentiality, integrity and availability of D/A information. Depending upon which services are implemented or activated, these additional threats can increase the device's vulnerability to interception, alteration, and injection of communications.

As shown in Figure 2: Common Mobile Threats and Mitigations, mobile devices, applications and infrastructure face a range of threats which have the potential to disrupt communications and business functions, and ultimately delay the full-scale adoption of mobile technologies in the Federal Government. These threats are constantly evolving and need to be addressed as mobile technology is adopted. The mitigation strategies identified to reduce the risk associated with these threats involve applying management, operational and technical controls to address threats to each element of the mobile architecture. In addition to the mitigations, management controls include security awareness training to address mobile-device specific threats and security policy defining rules of behavior and acceptable use of mobile devices.

Agencies should follow NIST guidance and implement a risk-based approach to identify, assess, and prioritize risks associated with mobile computing, and determine the likelihood and potential impact of these risks. Mitigation strategies and resources are then applied to defend against the most significant threats and reduce risk.

Element	Threat	Mitigation
Applications	Malware Exploitation of vulnerable apps Compromised apps Data/information leakage	App configuration management & monitoring D/A App Store, whitelisted/blacklisted apps Secure app development App wrapping App vetting and certification
Devices	Insecure configuration Vulnerable operating system Unauthorized access Virus/malware Loss of sensitive data Device loss/Theft	Device provisioning & management Mobile device integrity (Roots of Trust) Device password to unlock device Whitelisted/blacklisted apps, user training Encryption of data at rest (FIPS) Remote wipe of agency apps & data
Infrastructure: Agency Enterprise	Unauthorized access Virus/malware Data integrity Compromised apps Insecure coding	PIV-based user authentication Device authentication Device malware scan, integrity check & monitoring Signed apps & app verification Mobile app development & security vetting
Infrastructure: Access Networks	Eavesdropping, data interception Voice/Data collection over the air Drive-by downloads Location tracking (GPS) Behavior tracking	Encryption of data in transit (VPN) VPN, disable split tunneling & tethering User training and Rules of Behavior Device configuration profile Carrier SLA

Figure 2: Common Mobile Threats and Mitigations

Generic Mobile Computing Architecture

Integrating mobile computing capabilities into D/A's enterprise network requires leveraging existing infrastructure and adding new services and infrastructure. Existing infrastructure includes the Trusted Internet Connection (TIC), firewalls, intrusion detection systems, Virtual Private Network (VPN) gateways for authorized users, IAM repositories and mechanisms, and existing applications and services.

New services and infrastructure to be added for mobile computing include: MDM to ensure secure configuration, updates and allowed usage; secure development and lifecycle management of mobile applications, which may be hosted in a D/A or Federal Government app store; new methods for strong authentication of authorized users; data governance and standards for data tagging and security to enable data sharing; and NIST-validated cryptography to protect data. These are described below.

Mobile Device Management (MDM)

Because most commercially available mobile devices do not enforce security requirements to the extent required by an enterprise, MDM products have been developed to mitigate threats to mobile devices by enabling enterprise-controlled device configuration, security policy enforcement, compliance monitoring, and response (e.g., remotely lock and/or wipe a mobile device that has been reported as lost or stolen). MDM solutions typically include an enterprise server(s) component and an application installed on the mobile device to manage device configuration and security and report device status to the MDM.

Mobile Application Management (MAM)

Malicious or vulnerable mobile applications are a significant threat to mobile devices. This threat can be mitigated by following best practices for secure application development, and use of application whitelisting–which only allows installation of mobile applications from an authorized enterprise app store–and application blacklisting, which disallows installation of known vulnerable applications.

Mobile application management is a set of tools and processes that provide the ability to set up an enterprise application store, deploy mobile applications, provision and control access to internally developed and commercially available mobile applications, enforce application policy, monitor integrity and behavior of installed applications, and remotely upgrade or uninstall applications as necessary. As part of the mobile application lifecycle, the D/A should also develop a process for vetting mobile apps to check for vulnerabilities and malware, and digitally sign apps that have been approved.

Identity and Access Management (IAM)

Federal mandates[2] require use of Personal Identity Verification (PIV) credentials by Federal employees and contractors to access sensitive government information. Current smart card readers and standards for PIV

[2] Homeland Security Presidential Directive-12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004 and OMB M-11-11, Continued Implementation of Homeland Security Presidential

(footnote continued on next page)

or other two-factor authentication methods are expensive and difficult to implement on mobile devices. However, alternatives are available, such as readers that utilize the Bluetooth protocol instead of a Universal Serial Bus (USB) cable connection as well as select mobile device manufacturers that have developed and integrated PIV card reader "sleeves" for devices. Near Field Communication (NFC) is another option for wireless communication with a PIV credential, but its use requires revisions to the Federal Information Processing Standard (FIPS) standard for PIV. Work is underway on standards for NFC, PIV-derived credentials, and microSD Hardware Security Module (HSM) authentication methodologies.

Data Management

There are two aspects to data management: data categorization and tagging to enable information sharing and safeguarding; and encrypting sensitive information stored on a mobile device or transmitted across unsecured networks to protect against unauthorized access or disclosure. Policy on data governance and common standards for categorizing and tagging data need to be developed, to include guidance on interoperable tags for access control to Controlled Unclassified Information (CUI). In the meantime, the loss of a D/A-managed mobile device puts sensitive government information stored on the device at risk. Protection of sensitive D/A data requires use of FIPS-validated encryption modules. Some device manufacturers are undergoing the FIPS validation process for their devices, but there are very few modules currently available for mobile devices. This limits the number of mobile devices and/or MDM container solutions that meet Federal requirements for protection of data to a select number of devices and MDM vendors.

Federal Mobility Use Cases

To develop the DGS Barriers and Opportunities report, the MTTT identified five high-level user communities for digital government services. The communities were categorized into use cases ranging from Federal employees accessing classified information to citizens accessing public information published and hosted by the government. As shown in Figure 3: Federal Mobility Use Cases, the five use cases are separated into two broad scenarios, agency controlled and non-agency controlled devices.

There is an overlap between the agency and non-agency controlled scenarios where there is a separation of ownership/management of the information and applications specifically regarding Corporate-Owned Personally Enabled (COPE) and Bring Your Own Device (BYOD) device management options. There are two approaches to achieve this separation: devices built with two distinct environments, or software installed on the device to create a separate secure container for D/A data and applications. In the COPE device management model, the device is owned and managed by the D/A as Government Furnished Equipment (GFE), but personal use is allowed. Government information and applications are managed in a secure environment separate from the personal data and applications. In the BYOD model, the mobile device is

---

Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011.

personally owned by the user, who consents to installation of a secure government workspace on the device. Only the secure workspace is managed by the D/A to separate government data from the user's personal information and applications on the rest of the device.

The device management categories were further refined to reflect the sensitivity of information and the ongoing relationship between the user communities and D/A missions. The five mobility use cases were developed by applying the following criteria:

- Who is the user? (Which digital government user community?)
- What is the mission requirement for using mobile devices to access government information and services?
- What information is needed?
- What is the sensitivity and criticality (importance of timely delivery) of the information?
- Where is the user and where is the information?

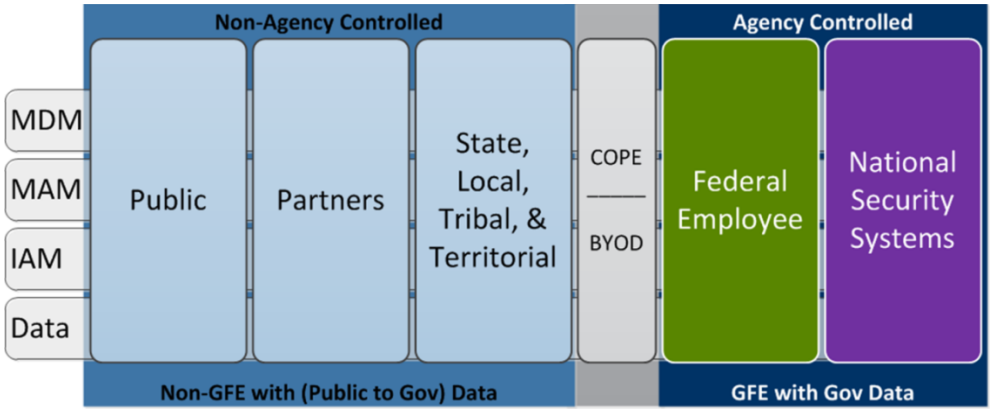


Figure 3: Federal Mobility Use Cases

The generalized mission requirement for all use cases is to meet the DGS objective: *Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.* Answers to the remaining questions are described below and summarized in Table 1: Federal Mobile Computing Use Cases.

Agency Controlled Mobile Devices

National Security Systems

This category includes Federal Government employees or contractors who require access to systems designated as national security systems to accomplish the mission, possess the necessary security clearances for access, and have a validated need to know. The highest level of data sensitivity is Top Secret. The user may be located in a D/A facility, with mobile access to the D/A's internal network, or working from a remote location external to the facility. The mobile device is fully managed by the D/A.

Federal Employee

Employees or contractors of a D/A using government networks comprise the Federal employee use case. This use case includes interactions within and between D/As (e.g., a Federal interagency task force). These users require access to D/A internal applications and information to meet mission needs. The applications may include services such as e-mail, calendar, contacts, voice; productivity applications for document creation, review, and editing; collaboration tools; and mission-specific applications and services. The highest level of sensitivity of information accessed is CUI. For some D/A missions, such as law enforcement and emergency response, expedient delivery of information to the employee may be critical for employee and public safety, and must be secured for evidentiary reasons. The user may be in the office, in the field, teleworking, or on travel (within or outside the U.S.). The data and applications to be accessed from mobile devices reside on government systems. Remote access with mobile devices will leverage the D/A's existing infrastructure and the mobile device is managed by the D/A.

Non-Agency Controlled Mobile Devices

State, Local, Tribal and Territorial

This use case includes state, local, tribal, and territorial government officials, law enforcement, fire service, emergency response personnel, and public health officials who are responsible for public safety. These entities share sensitive information with D/As for initiatives such as the National Sharing Strategy, State and Local Fusion Centers, National Suspicious Activity Reporting, infectious disease, emergency and disaster management. Trust agreements for two-way information sharing between D/As and these entities are specified through laws, Executive Orders, directives, or policies. Information shared may include non-Federal information, CUI, and unclassified information. Users are remote, and information may be located in D/A extranets, government internal systems, the D/A information sharing environment, or other Federal Government controlled data repositories. The mobile device is not managed by the D/A; it may be personally owned, issued by the user's employer or state/local government. Requirements for mobile device security, protection of information, and user authentication are imposed through policy and information sharing agreements.

Partners

Partners include contractors, financial institutions, suppliers, private industry, Federally funded research and development centers, national laboratories, academia, foreign governments, international agencies, or other organizations working for or with the Federal Government to support D/A missions. Information accessed may include CUI. In most cases, the requirements for protection of sensitive information are specified in contracts or information sharing agreements. For partners such as contractors or suppliers, compliance with security requirements is certified by the D/A and periodically audited. Users may be remote or on site at the government facility. Information may be located in D/A or partner extranets or internal systems. The mobile device is not managed by the D/A; it may be personally owned or issued and managed by the user's employer.

Public

This use case refers to American citizens, immigrants, and the general public who seek remote access to D/A information or services. D/A information is made available to the public; citizens' personal information associated with government benefits (e.g., Social Security, Medicare, disaster relief, immigration, or Veteran's benefits) is Personally Identifiable Information (PII) or Protected Health Information (PHI). Information collected from citizens for survey activities is also PII. Public information and services are available on D/A external websites, external facing data sources, commercial app stores or public-facing government app stores. Personal information related to government benefits is stored on internal systems with proxy services provided through the D/A's TIC infrastructure. Mobile devices are personally owned.

Table 1: Federal Mobile Computing Use Cases

Use Case	Information/Services Accessed	Information Sensitivity	User Location (Relative to Agency Facility)	Information Location	Device Control
National Security Systems	Secure voice, e-mail, calendar, contacts, mission-specific information and apps	Classified CUI Unclassified	Office, in the field, remote	Internal systems	Agency
Federal Employee	Voice, e-mail, calendar, contacts, government and agency information and apps, mission-specific information and apps	CUI Unclassified	Office, in the field, alternate work site, remote (CONUS or OCONUS)	Internal systems External systems	Agency
State, Local, Tribal, and Territorial	Information sharing sites and apps: public health, law enforcement, investigations, critical infrastructure, etc. (Trust relationship defined in policy)	CUI Non-Federal Unclassified Public	Remote	Information sharing environment Agency extranet	Non-agency Employer managed or Personally owned
Partners	Agency information and apps, e-mail, research information (Trust relationship specified in contractual agreements)	CUI Unclassified Public	On-site at agency facility, remote	Agency or partner extranet Internal systems	Non-agency Employer managed or Personally owned
Public	Public information, agency apps and services Personal information collected by the government or provided by the citizen	PII PHI Public	Remote	External sites Gov. application stores Agency extranet	Non-agency Personally owned

Mobile Security Reference Architecture

DHS' Federal Network Resilience (FNR) Division is responsible for developing reference architectures for Federal civilian agencies. FNR developed the Mobile Security Reference Architecture through a

collaborative interagency effort. This section presents an overview of the Reference Architecture; the full document is available from the DHS website.[3]

The Reference Architecture depicted in Figure 4: Mobile Security Reference Architecture presents the architectural components needed to provide secure mobile services to D/A user communities while providing the data confidentiality, integrity and availability critical to D/A mission success. It expands on the notional architecture shown in Figure 1: Generic Mobile Computing Architecture, and defines the mobile infrastructure and device management scenarios a D/A would need to support multiple use cases and a broad range of mobile applications and services. It describes the components of the mobile device infrastructure, which include MDM, MAM, IAM, and Data Management as well as VPNs, Intrusion Detection Systems, and the application and security gateways that mediate access from the mobility infrastructure to D/A enterprise information and services. Sample implementations are used to show how components of the Reference Architecture can be applied to address specific uses, such as public information services or fully managed GFE. Agencies may customize the Reference Architecture based on their business and operational deployment requirements by taking into account the associated risks and security implications.

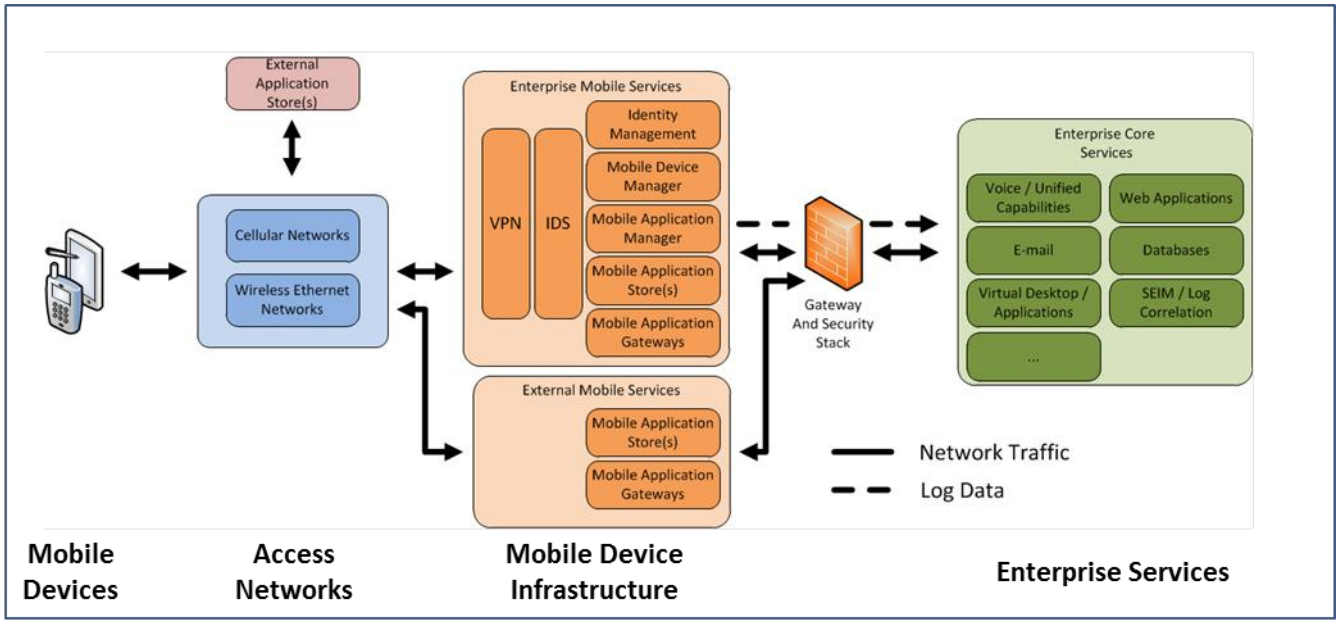


Figure 4: Mobile Security Reference Architecture

The Reference Architecture presents four mobile device management scenarios to meet different D/A operation and mission requirements (Figure 5). These scenarios map to the mobility use cases for D/A-managed and non-D/A managed devices described in the previous section of this document and cover a spectrum of controls from fully managed GFE to remote access from non-GFE devices.

[3] This document will be available at: *http://www.dhs.gov/network-and-infrastructure-security*.

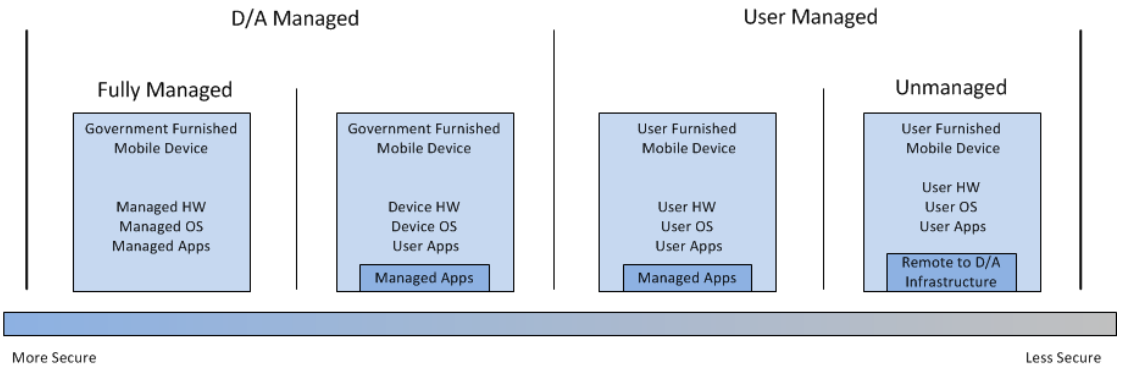


Figure 5: Reference Architecture Device Management Scenarios

Each scenario describes the associated level of trust and sensitivity of information processed and stored. Fully managed GFE mobile devices offer D/A the greatest control over service providers, device hardware selections, operating systems, applications (including version control), and policy control of additional features (e.g., camera and GPS). In this scenario, the mobile devices can be treated as an extension of the D/A's internal networks, and be granted access to more sensitive information than in other mobile device management scenarios. On the other hand, for the isolated applications on non-GFE mobile device scenario, agencies no longer have such controls so the mobile devices are limited to perform remote access via D/A VPN services for reduced business functionality (e.g., webmail and virtual desktop).

The Reference Architecture also presents a summary of security functions needed to manage mobile devices and the supporting infrastructure, and explains how to implement the security function for a solution. For instance, the configuration security function describes the appropriate logical and physical configuration settings necessary to deploy and maintain a secure mobile infrastructure. An appendix to the Reference Architecture maps these security functions to relevant NIST security control families. This mapping provides a high level summary of necessary security controls that complements, but does not replace, the mobile security baseline and overlays included as Appendix A to this document.

Other appendices to the Reference Architecture are: a more detailed description of mobile device security threats and guidelines for mitigating the threats; considerations for implementing mobile solutions in high risk environments; and a set of policy issues for D/A consideration. A Mobile Computing Decision Framework (i.e., hereafter referred to as the "Decision Framework") is included as a supplement to the Reference Architecture. The Decision Framework is intended to be used with the Federal mobility use cases and the corresponding security control overlays to help agencies select a deployment scenario to meet their mission, security, and operational requirements.

Federal Mobile Computing Security Baseline

Overview

A security baseline is a set of minimum security and privacy controls for Federal information systems and organizations based on security category of the information systems. It is implemented as part of the D/A's

organization-wide information security and privacy risk management process, and provides agencies with a consistent method to manage organizational risk and a common approach to security assessment, authorization, and continuous monitoring. NIST's Special Publication (SP) 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations,*[4] defines security controls for information and information systems categorized as low, moderate, or high impact per FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. These controls are based on every possible situation, for example, D/A information systems that are multi-user systems located in fixed physical facilities or locations.

Mobile computing presents security challenges not found in traditional fixed-location systems (e.g., desktop computers, workstations, servers) and laptop computers. As a class of computing devices, mobile devices and their management services are subject to some common PC threats and emerging mobile-specific threats. The increased risk from mobility must be considered when tailoring the baseline of security controls. Threats may be introduced by the user, the mobile device, applications, the Internet, other networks, or the wireless service provider. The threats present risk to the user, the device, information processed and/or stored on the device, and the D/A's enterprise information and services.

Mobile Security Baseline for Federal Employee Use Case

Using the guidance provided in NIST SP 800-53 Revision 4, the NIST baseline security controls for moderate impact systems have been tailored to the mobile environment for Federal employees accessing information and systems on a Federal network. This tailored baseline is specified as an 'overlay' for mobile computing to be utilized across the Federal Government. A security control overlay applies NIST or Committee on National Security Systems (CNSS) tailoring guidance to the security baseline to develop a set of controls for community-wide use for computing models such as mobile or cloud computing. An overlay is a combination of a full set of security controls, control enhancements, and supplemental guidance. The mobile security overlays tailor security controls to address threats and risks introduced by mobile devices and access to networks that are outside the direct control of the D/A. Supplemental guidance provides information and direction on how to apply the controls in the mobile computing environment. The mobile security baseline overlays address risk based on known threats to mobile computing; D/As must consider their threat environment as well as risk tolerance and select additional controls and/or control enhancements deemed necessary to meet their mission requirements in higher risk environments.

Securing the mobile environment involves multiple infrastructure elements: MDM, MAM, IAM, and Data Management. The combined set of security protections for each of these components comprises the overall mobile security baseline. However, with a consolidated mobile security baseline, it can be difficult for enterprises to ascertain which controls apply to each element. Therefore, the mobile security baseline

[4] NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. http://csrc.nist.gov/publications/PubsSPs.html.

will include MDM, MAM, IAM, and data management overlays tailored to each use case and each element of the mobile security architecture, as appropriate.

The mobile security baseline and overlays are developed through a consensus process by the MTTT's Federal mobile computing security baseline working group. The process of examining each control in the NIST baseline for applicability to mobile computing, developing specific rationale and guidance, and obtaining consensus from the Federal community on its inclusion in the mobile security baseline, is iterative and time consuming. To prioritize advancement of mobile capabilities and best serve the needs of the Federal community, the working group set the Federal employee use case as the highest priority for the mobile security baseline.

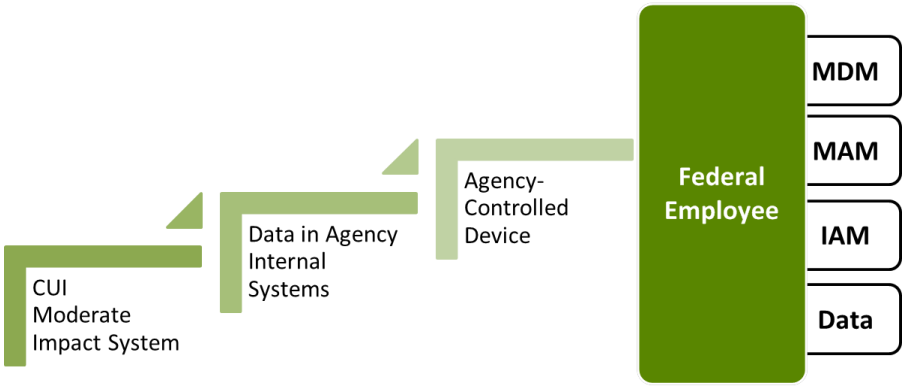


Figure 6: Federal Employee Use Case

The above Figure 6: Federal Employee Use Case, shows the Federal employee use case overlaid with the four key mobile architecture areas. The first priority for the mobile security baseline is MDM, since mobile devices with unknown configurations and security profiles present the most immediate threat to secure mobile computing. The initial draft of the MDM security controls identified functional security requirements for DGS Milestone Action 5.5, which tasked GSA with obtaining information and proposals for establishing a government-wide MDM platform consistent with the MDM overlay. The MAM and IAM security overlays have been developed next to address risks from malware and untrusted mobile applications and to set requirements for mobile device and user identification and access control, respectively. The MTTT technical working group considered developing a mobile device or mobile operating system (OS) overlay, but decided to concentrate on the four areas identified in the Barriers and Opportunities report. For guidance on securing mobile D/As can refer to the relevant Defense Information System Agency (DISA) Security Requirements Guides and Security Technical Implementation Guides[5] for guidance on securing mobile operating systems.

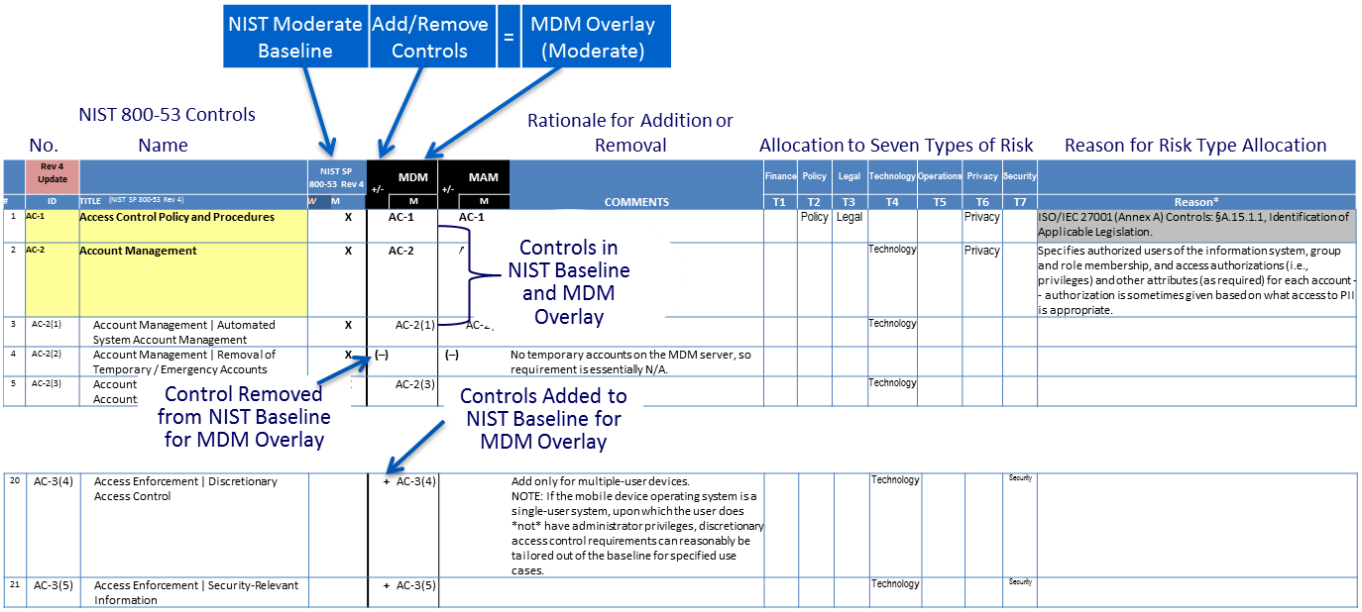
[5] http://iase.disa.mil/stigs/net_perimeter/wireless/smartphone.html

Because BYOD models are evolving and may quickly go beyond the scope of a D/A to control, future mobile security baselines may address the use case with a BYOD, but in order to discuss device entry into a government network, only GFE is considered in this document.

Appendix A, Mobile Computing Security Baseline contains the detailed moderate baseline for Federal employees, with defined controls for MDM and MAM, and notional controls for IAM and data management. The IAM and data management overlays will be further developed through the Federal CIO Council when the relevant standards are available.

Interpreting the Security Baseline

The Federal employee mobile security baseline maps the NIST SP 800-53 Rev 4 moderate baseline to the controls tailored for mobility. The overlay for each of the mobile infrastructure elements includes a column indicating controls that have been added to, or removed from, the NIST moderate baseline, with rationale for inclusion or exclusion of the control from the mobile security baseline. As shown in Figure 7: Interpreting the MDM Overlay, a plus sign ("+") indicates a supplemental control above the NIST SP 800-53 moderate baseline. A minus sign ("-") indicates the moderate control is not required and is removed from the overlay. The comments column provides rationale for inclusion or removal and additional guidance specific to mobile computing such as specific implementation guidelines. Detailed implementation guidance for the controls in the overlays is being developed and will be published by the Federal CIO Council.



#	Rev 4 Update	ID	TITLE (NIST SP 800-53 Rev 4)	NIST SP 800-53 Rev 4 W	NIST SP 800-53 Rev 4 M	MDM +/-	MDM M	MAM +/-	MAM M	COMMENTS	Finance T1	Policy T2	Legal T3	Technology T4	Operations T5	Privacy T6	Security T7	Reason*
1		AC-1	**Access Control Policy and Procedures**		X		AC-1		AC-1			Policy	Legal			Privacy		ISO/IEC 27001 (Annex A) Controls: §A.15.1.1, Identification of Applicable Legislation.
2		AC-2	**Account Management**		X		AC-2							Technology		Privacy		Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account - - authorization is sometimes given based on what access to PII is appropriate.
3		AC-2(1)	Account Management | Automated System Account Management		X		AC-2(1)		AC-2					Technology				
4		AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts		X		(-)		(-)	No temporary accounts on the MDM server, so requirement is essentially N/A.								
5		AC-2(3)	Account Account				AC-2(3)							Technology				
20		AC-3(4)	Access Enforcement | Discretionary Access Control				+ AC-3(4)			Add only for multiple-user devices. NOTE: If the mobile device operating system is a single-user system, upon which the user does *not* have administrator privileges, discretionary access control requirements can reasonably be tailored out of the baseline for specified use cases.				Technology			Security	
21		AC-3(5)	Access Enforcement | Security-Relevant Information				+ AC-3(5)							Technology			Security	

Figure 7: Interpreting the MDM Overlay

Agencies seeking to acquire MDM or MAM solutions to manage GFE mobile devices should use the appropriate overlay(s). Additional tailoring may be needed if additional overlays apply to the D/A network or system or to address unique circumstances in the D/A's environment. Care should be taken that security controls are not removed without a thorough understanding of the impact on the mission, environment and network. Removing one security control can affect different aspects of the mobility solution.

Additional Types of Risk

Information system-related security risks are only one type of risk the D/A needs to assess for an information technology (IT) investment. Other types of risk that are of concern to D/A include financial, policy, legal, technology, operations, and privacy. The NIST Risk Management Framework from NIST SP 800-37 describes information security risk management as one aspect of a holistic organizational risk management program that extends from the organization to the mission and ultimately to the information system level. To aid risk executives, CIOs, and Program Managers (PMs) in the risk-based tailoring process for their D/A, the mobile security baseline includes an allocation of the NIST security controls to these additional types of risk (ref. columns titled "Allocation to Seven Types of Risk" in Figure 7: Interpreting the MDM Overlay). Table 2: Mapping of NIST SP 800-53 Rev 4 Control Families to Type of Risk, shows how the 18 NIST SP 800-53 security control families are allocated to the different types of risk.

Table 2: Mapping of NIST SP 800-53 Rev 4 Control Families to Type of Risk

ID	Family	Financial	Policy	Legal	Technical	Operational	Privacy	Security
AC	Access Control		X	X	X		X	X
AT	Awareness and Training		X	X	X	X		
AU	Audit and Accountability		X	X	X		X	X
CA	Security Assessment and Authorization		X	X	X	X		
CM	Configuration Management		X	X	X	X		X
CP	Contingency Planning		X	X	X	X		
IA	Identification and Authentication		X	X	X			X
IR	Incident Response		X	X	X	X		X
MA	Maintenance	X	X	X	X	X		X
MP	Media Protection		X	X	X	X		X
PE	Physical and Environmental Protection		X	X	X	X		X
PL	Planning		X	X	X	X		
PS	Personnel Security		X	X	X	X		
RA	Risk Assessment		X	X	X			X
SA	System and Services Acquisition	X	X	X	X	X		X
SC	System and Communications Protection		X	X	X		X	X
SI	System and Information Integrity		X	X	X	X		X
PM	Program Management		X	X	X	X		

While this mapping considers only information security controls, risk executives can use these allocations to decide if each type of risk has been adequately addressed per the D/A's risk management strategy. For example, System and Services Acquisition (SA) controls have obvious financial (acquisition) and policy implications, which should trigger consideration of investment sources (e.g., build vs. buy, outsourcing, and contract vehicles). Access Control 8 (AC-8), System Use Notification, has policy, legal, privacy and technology implications.

The Decision Framework and the mobile security baseline contain considerations and references on how to address the risk areas. The rightmost "Reasons" column (Figure 7: Interpreting the MDM Overlay, "Reason for Risk Type Allocation") of the mobile security baseline also provides references and directions to address the risk areas and guide risk decisions. The Decision Framework includes guidance and example questions as a starting point for consideration for each type of risk (Table 3: Example Legal and Policy Risk-Related Questions from Decision Framework). This information can help the risk executive identify where gaps may exist that might need additional consideration or acceptance of risk. Plotted out, the overall diagram should communicate all the areas of risk the owner must consider when choosing to accept risk, mitigate, or not implement a mobile solution.

Table 3: Example Legal and Policy Risk-Related Questions from Decision Framework

Legal Risk
Ask the following basic questions when evaluating legal risks: • What sort of Rules of Behavior and monitoring policies will be necessary to both inform users of their expected behavior and to serve as a basis for legal or employment actions against violators? • What sort of use agreement will be necessary to inform users of the remote wipe policies (including what data will be wiped)? • What documentation of consent may be needed or required before the organization can monitor or search an employee's device? • What capabilities does the solution have to support e-discovery and data-retention to satisfy Freedom of Information Act (FOIA) and other legal requirements? • Do the solution's communications providers have their own e-discovery, data retention, and data breach notification policies for Short Message Service (SMS) messages, call history, voicemail, etc.? • How will data management, retention and disposition be addressed throughout the lifecycle of the mobile device?
Policy Risks
Ask the following basic questions when evaluating policy risks: • To what extent will the organization require control over their mobile devices? • Who owns the information that resides on the devices? • How does the organization want to define what organizational information is allowed to be stored on the device? How would the policy be enforced? • What types of personalization are mobile device users allowed to perform?

Using the Mobile Computing Decision Framework to Select a Mobile Solution Architecture

To guide D/As in defining mobility requirements and selecting a mobile architecture, the Reference Architecture includes a Decision Framework, depicted in Figure 8: Mobile Computing Decision Framework Graphic. The Decision Framework describes an approach for risk analysis and prioritization of business decisions regarding mobile solutions, enabling D/As to make informed decisions when assessing the risks of mobile solutions. The starting point for the Decision Framework is identification of the relevant Federal mobility use case(s). A mobility mission requirement may involve only a single group of users (e.g., Federal employees) or may span multiple use cases – employees, partners, state/local/tribal/territorial, and the public. Organizations considering the deployment of mobile devices within their organization have many decisions to make. These decisions include (but are not limited to): how mobile technology will support the organization's mission, what platforms to support, what technologies will be used to support mobile devices, what applications to deploy, and who will manage the solution. The Framework describes a four-stage process to define a specific business case, examine risks and tradeoffs, and reach a decision on mobile applications, devices and infrastructure elements:

- Define the mission requirement with a use case that describes users, information sources and sensitivity, and location of use;
- Identify the balance between three primary drivers: capabilities, cost and security;
- Assess risk (policy, legal, privacy, financial, technical, security, operational); and
- Select the mobile computing environment: applications, device, and infrastructure.

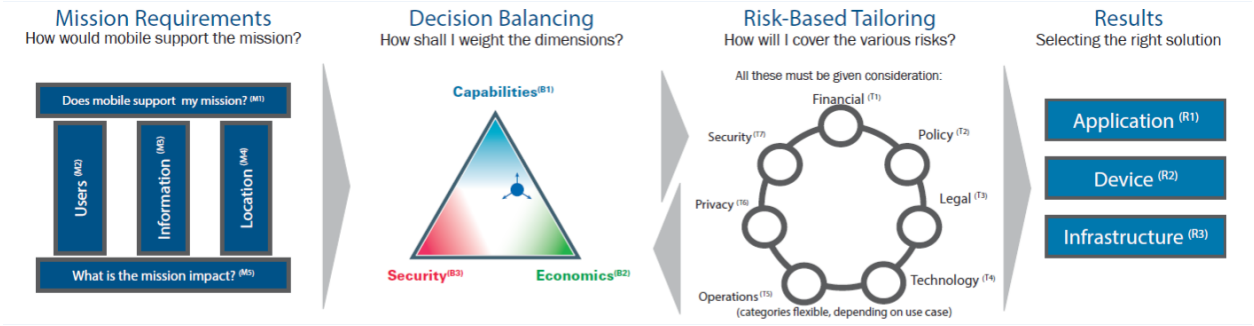


Figure 8: Mobile Computing Decision Framework Graphic

This section demonstrates how to use the Decision Framework for the Federal employee use case, resulting in decisions on implementation of the Reference Architecture and mobile security baseline. The first stage in the Decision Framework defines the D/A's mission need for mobile computing. The sample business case described below is a generalized example only; it does not reflect a Federal employee business case for a specific D/A, and example results should not be construed as requirements. It explains how to balance security, capabilities and cost, how to tailor security controls to address risk in accordance with the organization's risk management strategy and risk tolerance, and the resulting decision for a mobile solution.

Example Mobile Computing Business Case

Stage 1: Mission Requirements

Overview

The mobile computing decision process begins with a mission requirement for mobile computing. It should include a well-defined business case that describes users, information sources, information sensitivity and criticality, and location of use. In essence, the Mission Requirements stage helps the organization build a use case for mobile computing by establishing "who needs access to what, what is the sensitivity and criticality of the information, where is the information located, where do they need access to it, and why?" An organization must understand the needs of the personnel (both internal and external to the organization) who support the mission, the information they must access, their roles, the physical location, environmental factors, and mission criticality under which the information must be accessed. The outcome of this stage is a preliminary assessment of mission impact – whether use of mobile technologies would benefit the D/A's mission.

Sample Federal Employee Business Case

Federal employees who spend a majority of their work time in the field require remote mobile access to D/A information and services, such as e-mail, the D/A's web-based productivity and collaboration applications, and mission-specific mobile applications and forms. The current process for entering mission-specific information from remote locations is manual and error-prone, and information cannot be uploaded to D/A systems until employees are in an office location. This impacts productivity and can result in inaccurate and out-of-date information. Employees have used the real-time mapping and location services capabilities of their personal mobile devices to facilitate movement in their job performance. Some employees have GFE devices but these devices support only e-mail and limited web browser access. Because the currently available applications and location information are limited to office locations, employees often seek approval to either use their personal devices to enhance their mission capabilities or use issued GFE devices that provide these applications and services.

The D/A's PM assesses the request for mobile devices and determines that using mobile technologies will benefit the mission and enhance employee productivity.

Stage 2: Balancing Security, Capabilities and Cost

Overview

Three dimensions influence implementation of mobile technologies – mobile computing capabilities, economics (cost), and security. An organization reaches the Decision Balancing stage (Figure 9: Decision Balancing) when it has established a sufficient need to implement a mobile solution for a given mission. However, implementing the solution entails trade-offs, determined by the mission requirements, among the

Figure 9: Decision Balancing

following three major areas of consideration:

- Security—how the information must be secured;
- Capabilities—what an authorized user must be able to do with the information;
- Economics—how much an organization can afford to spend to obtain the desired security; and capabilities, and how can it leverage existing capabilities.

Sample Federal Employee Business Case

For this example business case, the PM identifies the capabilities that are the driving factors to improve employee productivity, access to information, and the ability to respond quickly to changing situations in the field. The balancing factor is security: the desired capabilities include processing of CUI and PII, which must be protected per Federal requirements. The control factor is cost: the ability to maximize capabilities with adequate security protections while maintaining best value in the D/A economic environment. The PM asks the D/A Chief Information Security Officer (CISO) to conduct a high-level risk assessment of the systems, data and applications identified in the mobile technology request. The CISO determines that the systems are moderate impact level which include CUI and PII data, and selects the Moderate impact mobile security baseline for Federal employees as security requirements for the requested capabilities.

The business case requested consideration of personally owned devices or GFE. Although the PM and CISO believe that the devices will need to be GFE to meet security requirements, use of BYOD is not ruled out at this stage. The PM provides the business case information, the PM's assessment of the request and balance point, and the moderate mobile security baseline to the D/A risk executive, and asks the risk executive to consider both options during the next stage in the process.

Stage 3: Risk-Based Tailoring

Overview

Using the relative importance of security, capabilities, and economics as determined in the previous stage, the risk executive can utilize NIST SP 800-39, *Managing Information Security Risk*, to help identify risks in each of the seven risk categories. Example considerations for each type of risk are:

- Financial – investment sources, acquisition vehicles, consumer technologies, rapidly evolving technology, provisioning cost, operational cost, replacement and upgrade cost, supply chain risk management;
- Policy –security policy, monitoring, compliance enforcement, security awareness training, social media policy, mobile device policy and acceptable use/rules of behavior;
- Legal – lost devices, copyright/unlicensed applications, remote wipe of devices that contain mixed personal and government data, reimbursement for personal device use, archiving requirements, discoverability, data ownership, employee monitoring, labor unions and expectations of availability during non-work hours, retention requirements for text messages;
- Technology – market risk, interoperability, mobility and network infrastructure, technical standards, virtual desktop infrastructure (VDI), application store, migration/development of applications and services for multiple platforms, management of devices, applications and content;

- Operations – training and staffing of personnel for development and management of mobile computing assets (hardware, software and infrastructure), help desk support, network operations, impact of mobile usage on infrastructure (e.g., bandwidth);
- Privacy – separation of personal and government data, processing and storage of PII, Geolocation services and monitoring, device "find me" technology, and remote wipe. See DGS report, Recommendations for Standardized Implementation of Digital Privacy Controls,[6] for information on meeting privacy obligations under the DGS; and
- Security – device management, device and user authentication, protection of data at rest and in transit (encryption), application whitelisting and blacklisting, security and software updates, device integrity checking.

Each D/A should conduct a risk analysis to identify the risks and evaluate the impact that implementing mobile computing will have on the organization. These risks apply to mobile devices, devices with their associated security and infrastructure, the applications and data accessed with mobile devices, and the entire D/A enterprise. Risks may be assessed by a D/A-specified risk assessment procedure, if available, or by use of NIST SP-800-30 Revision 1.[7] The risk assessment procedure may produce quantitative (numerical value) or qualitative (low, medium/moderate, high) risk levels that reflect the organizational tolerance for risk. The CIO, PM, or risk executive can use the Decision Framework's Risk-Based Tailoring tool (Figure 10: Risk-Based Tailoring) to identify risk types.

Figure 10: Risk-Based Tailoring

Sample Federal Employee Business Case

Figure 11: Example Risk-Based Tailoring Results – BYOD Option, represents the risk executive's assessment of the BYOD option for the business case. The risk executive has made a preliminary determination that D/A infrastructure and operational support capabilities will adequately address technical and operational risk for either the GFE or BYOD device management option. However, the risk executive concludes that use of personally owned devices for D/A business presents significant policy, security, privacy, legal, and financial risk. This imbalance in the ability to address risks will result in a change in the initial weighting of the dimensions (e.g., capabilities, economics, security) described in Stage 2. The D/A may have an allocated budget for mobility, but needs to determine a viable solution to support the mission need. If the cost to implement the desired combination of capabilities and security is deemed too high, then economics is given a higher weight, which affects the balance with the other two dimensions, security and capabilities.

---

[6] Recommendations for Standardized Implementation of Digital Privacy Controls, December 2012, available at: https://cio.gov/wp-content/uploads/downloads/2012/12/Standardized_Digital_Privacy_Controls.pdf.

[7] NIST 800-30, Revision 1, Guide for Conducting Risk Assessments, September 2012, available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

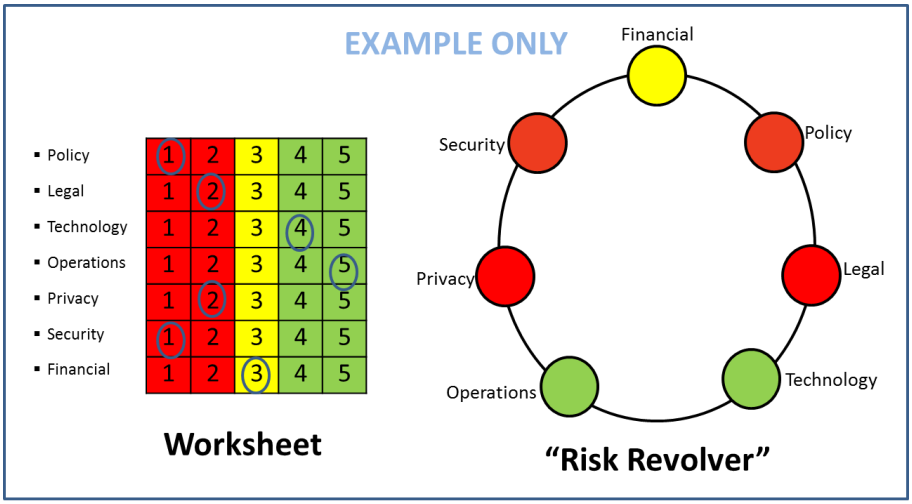


Figure 11: Example Risk-Based Tailoring Results – BYOD Option

The risk executive presents the assessment to the PM. In this example, to reduce the assessed risk of using BYOD, the PM reconsiders the decision balance, assigns security a higher weight, and reduces the weighting of capabilities. To mitigate the identified risks, the PM considers offering minimal capabilities such as virtual desktop access and web-based applications in a BYOD model. However, intermittent wireless network connectivity and the need for employees to have access to mission-specific applications when there is no wireless signal makes this option infeasible for the defined business case.

This balancing process, comprising Stages 2 and 3, should be followed iteratively until the final decision is reached incorporating acceptable risk, reasonable costs, and a high probability of building the required mobile capabilities in a timely and efficient manner. At the end, the D/A may accept a certain amount of risk, depending on D/A risk tolerance.

The PM re-adjusts the decision balance to its original point, and asks the risk executive to assess the managed GFE model. The risk executive then assesses controls for each of the seven types of risk for the GFE option and arrives at the diagram in Figure 12: Example Risk-Based Tailoring Results – Fully Managed GFE Option. In this example, policy risk is not fully addressed (i.e., it is assessed as yellow rather than green) because the D/A needs to document and communicate its mobile device policy and rules of behavior; legal risk is not green because the D/A needs to address union concerns about expectations for after-hours work if union employees carry the mobile devices.

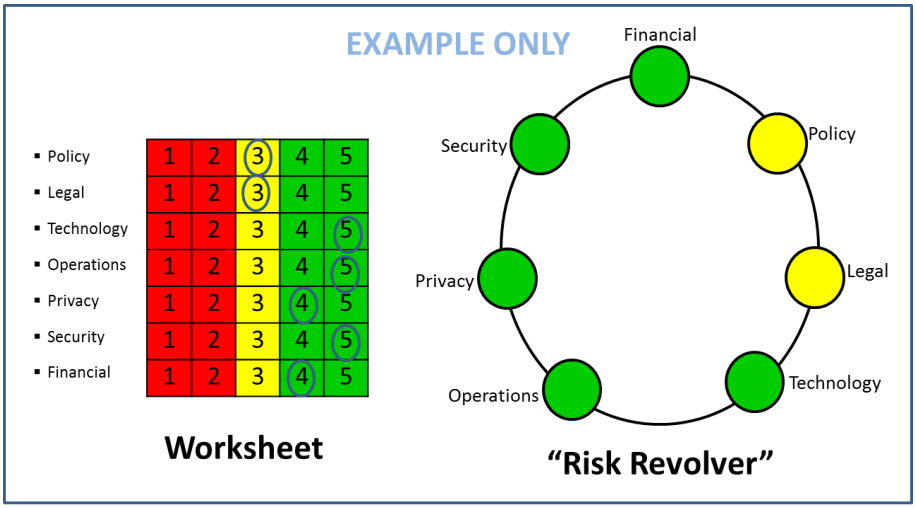


Figure 12: Example Risk-Based Tailoring Results – Fully Managed GFE Option

Stage 4: Results

Overview

The Decision Balancing and Risk-Based Tailoring stages help D/As define requirements and risk tolerance, resulting in guidelines and considerations on how to position a mobile computing solution within the enterprise. Utilizing those guidelines and considerations, the organization should be able to determine what aspects of infrastructure, mobile devices, and applications will benefit a given organizational mission. Based on decisions made through Stage 3 of the Decision Framework, the D/A can select the Reference Architecture implementation that best meets its business and security requirements, and identify the security control overlays (e.g., MDM, MAM, IAM, data management) that must be addressed in its mobile security architecture.

Sample Federal Employee Business Case

After the second iteration of decision balancing and tailoring risk, the D/A has determined the risk of allowing employees to use personally owned devices outweighs mission benefit, and decides the only acceptable option is to procure and provision mobile devices that are fully managed by the D/A. Figure 13: Fully Managed GFE Example from the Reference Architecture depicts the high-level implementation for a fully managed GFE mobile device. For the sample business case, all mobile security overlays (e.g., MDM, MAM, IAM, and Data Management) apply. Details on each element of the mobile architecture (e.g., device, applications, and infrastructure) follow.

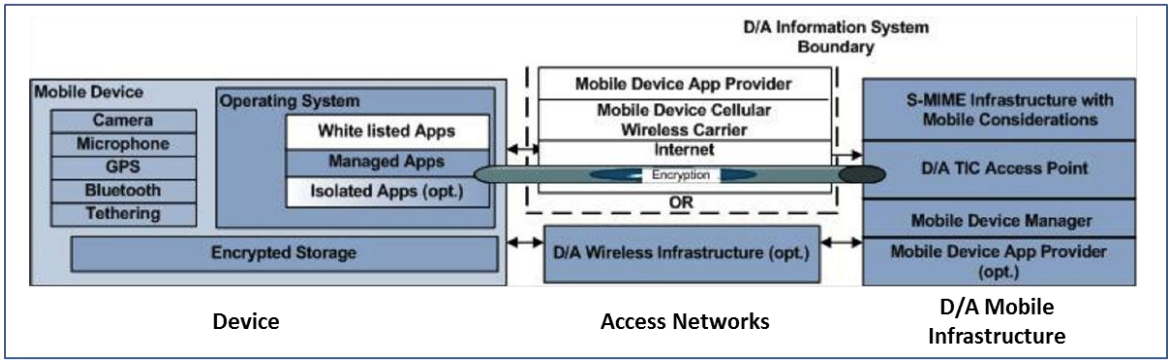


Figure 13: Fully Managed GFE Example

Mobile Device

Based on the requirements and risk-based tailoring decisions made in Stage 3, Risk-Based Tailoring, the D/A determines that the mobile device will be GFE. The PM expresses a preference for more than one mobile operating system, and both smartphone and tablet options. Since the device will be used outdoors, it must work well in bright sunlight, heat and cold. The device must be secure by design (i.e., it must implement "roots of trust" and monitor and enforce its security and integrity consistent with the Enduring Security Framework and NIST guidelines for mobile device integrity). The device security functions must be made available to the mobile operating system to ensure applications and services (including MDM) can use these functions. An MDM solution will be required to manage device provisioning, integrity, configuration profiles, interfaces, applications, and services. The MDM will enforce authentication requirements to protect against unauthorized access to the device and installed applications and services. The device must support PIV authentication to enterprise systems and services, and sensitive data at rest will be encrypted with FIPS 140-2 validated encryption modules, with configuration assured by mobile device integrity mechanisms. Data communications to the enterprise infrastructure must be secured through a VPN service that employs FIPS 140-2 validated cryptography. Productivity and mission critical applications will be installed during device provisioning, and additional applications will be available from the D/A-specific or Federal Government app marketplace; only allowed (whitelisted) applications may be installed post-provisioning.

Applications

Due to the nature of their work, employees will use the mobile device rather than a laptop or workstation for most of their computing needs. To meet needs for ease of use, the D/A will provide existing enterprise services (e.g., e-mail, calendar, contacts) through the device's native capabilities rather than providing mobile versions of these and other productivity applications. The D/A will provide software for document viewing and editing either through native device capabilities or with mobile versions of existing applications, and will need to develop or migrate mission-specific applications to mobile platforms. The mobile applications will be managed by a MAM solution.

Infrastructure

The D/A will need to address performance, scalability, availability, and reliability of its existing infrastructure to support mobile users, and needs to acquire MDM and MAM solutions (on premise or outsourced), and implement mobile authentication solutions and data management that include the following functionality:

- **Device Management**—The MDM provisions, manages and monitors device integrity and compliance with the D/A's security policy prior to allowing access to enterprise services. If a managed mobile device is lost or stolen, the MDM solution can remotely lock the device and/or erase (wipe) D/A applications and data. Provisioning includes issuing a device credential, disabling unneeded interfaces or services and setting other configuration parameters (e.g., password, screen lock, camera enabled/disabled, etc.), installation of any applications required for network connectivity, setting up user accounts, installing certificates, installing D/A-approved applications and services and anti-virus software, if available. The MDM solution will install updates (e.g., operating system or firmware) "over the air" for all devices, and perform configuration changes remotely. The D/A uses the Moderate MDM security control overlay tailoring to include application whitelisting.
- **Application Management**—To manage and secure mobile applications, the D/A will need to establish guidelines and an environment for mobile application development and testing, and develop a process to vet, certify and sign approved apps. A MAM solution (product or service) will be required for mobile application management, monitoring, and distribution to D/A, government, or allowed public application stores. The MAM will need to interface with the MDM to provide app whitelisting and blacklisting services, and to provide apps and updates for installation on managed mobile devices. PIV authentication is required for remote access to CUI or mission-specific applications or data; so the MAM solution will need to interface with the D/A's existing IAM services. The D/A applies the Moderate MAM security control overlay with D/A additional enhancements for application testing and evaluation, if required.
- **User Authentication** — Solutions for mobile authentication (including PIV credentials) will need to be implemented within the IAM infrastructure; these include provisioning support for user credentials which may be stored on a FIPS 140-2 validated internal or external (e.g., microSD Hardware Security Module) cryptographic tokens. The D/A FIPS 140-2 VPN connections from mobile users will terminate at the D/A's VPN or other access control gateway; the gateway will need to authenticate both the user and the device.
- **Data Management** —The D/A will need to ensure CUI data is appropriately categorized, tagged and managed to support delivery of the right information to the right users at the right time.

Example Results for Other Use Cases

Although the current version of the mobile security baseline focuses on the Federal employee use case, the government will continue to develop security guidance for its interactions with the public and other user communities. From the separation of use cases into D/A managed and unmanaged device scenarios and the example implementations described in the Reference Architecture, some assumptions can be made

regarding MDM, MAM, IAM, and data management for other use cases. The following sections represent these general assumptions.

National Security Systems

Security requirements for National Security Systems are defined by the Committee on National Security Systems, and therefore outside the scope of this document. For information on mobile security for national security systems, see http://www.nsa.gov/ia/programs/mobility_program/index.shtml.

State, Local, Tribal, and Territorial

D/As cannot control the configuration or type of device used to access government information, but can impose security requirements through policy and information sharing agreements. Devices used by state, local, tribal, or territorial officials may be provided by the D/A as GFE, may be issued and configured by the organization such as corporate furnished equipment (CFE) or may be owned by the user. Many of the remote access requirements imposed on these users are the same for a mobile device as for a laptop or workstation: user authentication to the device, VPN encryption of all communications, user identification and authentication to D/A systems, secure e-mail, and restrictions on storage of sensitive information. If feasible, prior to allowing access to D/A services, the D/A should check the integrity of the mobile device's operating system, and deny access if the device's operating system has been compromised (e.g., jailbroken or rooted). D/As may require that both the device and the user be authenticated. If so, the D/A will need to specify which devices it supports, enroll the devices in the MDM and issue a device certificate for authentication. The D/A will need to ensure that data is appropriately categorized, tagged and managed for release. Users may have multiple roles within a mission area (e.g., for law enforcement or emergency services missions), which requires granular role-based access control for information sharing.

Partners

D/As cannot control the configuration or type of device used by partners, but may limit support for mobile apps or web applications to a limited number of device types and operating system versions. The device is CFE with requirements contractually imposed to protect access to the device and data. Agency requirements for user authentication to the device and D/A systems, encryption of data at rest and in transit, and device integrity checking are similar to the State, Local, Tribal and Territorial use case. However, the D/A may contractually require additional controls to secure information and D/A applications, and audit the partner for compliance. To minimize the risk of malware being introduced into D/A systems from an infected (illegal) mobile device, the D/A could deploy functionality to check if the user has illegally altered the device's security protections to install applications and services that are not allowed by the device vendor. In some cases, partner personnel (e.g., contractors, law enforcement or inspection personnel) are issued and operate GFE mobile devices in addition to their CFE or personal device. In these situations, the GFE devices are managed and controlled by the D/A as described under the Federal employee use case. This use case has the same requirements for data categorization, tagging and access control as the previous use case.

Public

D/As cannot dictate or control the type of mobile device or operating system the public uses to access government information and services, nor can D/As restrict the applications and services used on the device. The D/A will need to tailor the data management overlay to ensure data released to the public is correctly categorized. This includes a means to assure the accuracy and integrity of critical public health and public safety data, e.g., epidemics, natural disasters or public emergency information. To maintain the public trust, the D/A should consider mechanisms to provide data assurance, such as information or data branding or an approval/certification process for third-party applications that use such critical public health and safety D/A data.

For access to personalized information (e.g., application for benefits), the D/A will need to tailor the IAM and data overlays to identify the user and the data the user can access. For public applications and services, several types of authentication levels will likely be supported: none, anonymous (e.g., to indicate that the user is a member of a particular group such as veterans), user id and password previously registered with the D/A, or a credential issued by a third-party identity provider by a trust framework provider approved under the Federal Identity, Credential and Access Management initiative.

Conclusion

The DGS challenges D/As to "deliver and receive digital information and services anytime, anywhere and on any device" and to "adopt a coordinated approach to ensure privacy and security in a digital age." This release of the mobile security baseline and Reference Architecture represent the Federal Government's first steps to set government-wide standards and guidelines for secure mobile computing. By implementing the mobile security baseline and Reference Architecture, D/As will be better able to address threats and vulnerabilities mobile devices can introduce into a government computing environment.

These are first steps only. The mobile security baseline and Reference Architecture reflect the current state of D/A infrastructure, data, and services, and the reality that standards and practices for IAM and data management are emerging. The Federal CIO Council will continue to develop the security baseline to further refine security controls for IAM and data management. Future versions of the mobile security baseline and Reference Architecture will focus on securing the data instead of the device, ensuring data is only shared with authorized users, and defining security considerations for the public, partner, and state/local/tribal/territorial government use cases. Subsequent versions of the Reference Architecture will incorporate updated solutions in areas such as continuous monitoring, cryptography, and IAM that support the shift to securing the data itself (including provenance, audit, and distribution control).

Appendix A: Federal Mobile Computing Security Baseline

The “Intro” tab of the baseline gives instructions and information on the format and content of the mobile security baseline. The “Baselines” tab contains the MDM and MAM security controls for the Moderate mobile security baseline in the “MDM” and “MAM” columns, respectively. Controls included in the “IAM” and “Data” columns are notional. The MTTT will continue to refine the mobile security baseline to include these elements.

Appendix B: Mobile Security Technical Exchange Meetings (TEM)

Mobile Security TEM, March 11-12, 2013

The Federal CIO Council's Information Security and Identity Management Committee (ISIMC) hosted a Mobile Security TEM in March 2013 to discuss how mobility transforms the ways that D/As accomplish their missions and its impact across use cases (national security systems, Federal employees, state/local/tribal/territorial, partners, and the public). The focus of the TEM was to clarify and identify risks and gaps that need to be addressed in the DGS 9.1 deliverables. To gain better insight into how D/As address mobility across a mission area, the ISIMC organized the TEM to examine mobility as communities of interest, which span multiple use cases. Emergency Support Services, for example may include Federal employees, state/local/tribal/territorial, domestic and international partners, and the public. TEM working groups were formed to examine risks and gaps by these communities of interest:

- **Citizen Services (CS)** – User groups are providers of government information/services such as: weather alerts, traffic alerts, airline information, and Social Security and grants;
- **Emergency Support Services (ESS)** – Systems, apps, and infrastructure used during natural disasters and emergencies. Users include first responders, disaster relief teams, and law enforcement;
- **Financial (FIN)** – User groups that provide secure financial information include finance officers, financial institutions, tax preparers and processors, and financial auditors;
- **Health/Medical (MED)** – User groups are health care providers, researchers, and the issuers of medical alerts and information who provide health information, service provisioning, and life-saving capabilities while protecting the privacy of patient information;
- **Law Enforcement (LE)** – User groups include Federal, state, county, city, tribal, and international law enforcement agencies that use mobile technologies to support mission capabilities and to provide interoperable communications among the law enforcement community; and
- **National Security (NS)** – User groups include national command authority, senior leader communications, National Security Council, and other communities supporting national security.

Each working group used the Decision Framework to assess gaps and risks, and presented their findings to all TEM participants. The working groups recommended changes and additions to the Decision Framework and identified the top risk areas and risk considerations for their community of interest.

Comments on Mobile Computing Decision Framework

- Clarify that the expected user of the Decision Framework is the program manager, CIO or risk executive, not the end user of the mobile technology;
- Modify scope of the most appropriate level to use the Decision Framework – it works best at the project rather than program level;
- Add time element between user and location (e.g., criticality and timeliness of information for officer safety or for emergency response);

- For information that is provided to the public (e.g., CS, MED), there are two general applications: collection of information from the public and dissemination of information to the public and requirements and assessment of risk differs for these applications;
- The initial requirement for mobile solutions may come from partners or the public who push the Federal community to develop/deliver mobile apps;
- Refinements to description of Information/Data,
  - Any shared data/database must have granular vetting and must be properly mapped back to owner,
  - Auditability and data retention are extremely important for local LE,
  - Address the importance of data tagging,
  - Use of social media plays a large role in delivery and receipt of information during emergency situations; however, this presents an issue with the reliability and accuracy of the information;
- Refinements to description of Users,
  - Require Multiple Identification Capabilities,
  - Officer/Watch Commander/Lead Investigator (Role Based) – one user may have multiple roles (true for LE and ESS); and
- Results section needs more explanation to guide PM decisions.

Comments/Considerations on Types of Risk

The following list of considerations and gaps is intended to aid D/As in identifying and addressing the different types of risk. The user communities identified the top risk areas for their community of interest. These rankings are noted in parentheses, where (CS, ESS, LE) indicates that this type of risk was a top concern for the Citizen Services, Emergency Support Services and Law Enforcement communities.

Policy (FIN, MED, LE)

- Importance of protocols, Chain of Command;
- Defining who is eligible to participate in a BYOD program and responsibilities for hardware upgrade, whether user has to remain in the program for a period of time;
- Data governance – quality, integrity and data provenance;
- Auditability and data retention;
- Issuance of wireless device to foreign nationals (policy and legal risk); and
- Inability of D/A policy to keep up with the pace of technology change.

Legal (CS, NS)

- For data collection from the public, D/As need to consider who binds the D/A to the End User License Agreement;
- Dissemination of data in public places, an extra burden to protect data to ensure its authenticity;
- Increased risk to D/A brand integrity with citizen data; and
- Application developer licenses and ramifications of sharing in-house developed apps with Federal Government (in a Federal Government app store).

Privacy (CS, ESS, FIN, MED)

- For mixed personal/government use: concern about which user ID is used to load apps on a device;
- Data dissemination, consent from individual to use their information (even if anonymous);
- Next of kin Notification in emergency situations (e.g., homes destroyed) before it's news; and
- Notifying citizens about collection and use of information they provide (e.g., for surveys).

Financial (FIN, NS)

- Remuneration in case of spillage on personal device;
- Staffing implications;
- Supply chain risk management; and
- Data plans.

Technology (CS, FIN, LE, NS)

- For some communities (e.g., LE), location services must be controllable, centralized and secure for officer safety reasons;
- Device battery needs to last a full shift (GPS drains battery);
- 508 compliance (e.g., alternate input methods);
- Quality of Service is important for video and secure voice; and
- No government data priority program on cellular network similar to GETS.

Operations (ESS, LE)

- Support/retraining;
- Lack of training, lack of planning on how to use infrastructure;
- Lack of resilient infrastructure;
- Use of social media/crowdsourcing data to identify where additional resources are needed;
- Spatial analysis on criminal activity;
- Officer safety; and
- Need for applications that work without a signal such as maps and situation reports.

Security (CS, ESS, MED, LE, NS)

- Risk of PII data loss;
- Need for Secure Bluetooth;
- Risk of unknown/rogue Wi-Fi access points;
- Concern about cellular carriers pushing updates to mobile devices;
- Need for role-based information sharing and flexible authentication options to support users who have different roles in a particular community (e.g., LE, ESS);
- Considerations for release of information/Data dissemination,
    - ID proofing before allowing access to citizen PII or PHI,
    - Critical infrastructure and information integrity (e.g., GPS spoofing); and
- Need for a central government clearing house for vetting apps and mobile device updates.

Federal Mobile Security: Moving From Barriers to Baselines, April 17, 2013

At the request of the Federal CIO Council's Mobile Technology Tiger Team (MTTT), the American Council for Technology-Industry Advisory Council (ACT- IAC), Tech America, and the Armed Forces Communications and Electronics Association (AFCEA) hosted a Mobility Forum in Washington, D.C. to solicit feedback from industry on the content of published and in-process mobile security documents developed for DGS Milestones 5.5, 9.1 and 10.2. The forum explored the intersection of a Federal case study in the four key mobile areas: MDM, MAM, IAM, and Data Management.

The conference began with a Federal executive panel representing the Chief Information Officers of DHS, DoJ and DoD, who presented their views on deploying mobile technology. The agencies expressed a commitment to deploying mobile technology to meet mission needs, but stressed the need to make sure the technology is secure and that privacy issues are addressed.

The MTTT briefed the forum participants on the progress on three deliverables for mobile security: the GSA Request for Technical Capabilities for its Managed Mobility Program; the Mobile Computing Security Baseline, and the Mobile Security Reference Architecture, which includes a Mobile Computing Decision Framework. Industry representatives were provided with the latest versions of these documents and asked to provide verbal feedback at the Forum and to submit written feedback.

During a roundtable session, industry members provided feedback on government adoption of mobile technology, focused on the Federal use case and the four key areas for enterprise mobility management. Industry members included representatives from the telecommunications industry, defense contractors, mobile technology industry, and other companies. The session was separated into two topic areas: MDM and Data and MAM and IAM. Themes and comments from industry included:

- Don't apply desktop oriented security frameworks to a mobile scenario. MDM requirements influenced by legacy OS security capabilities;
- The overlay may be a little heavy and a more simplistic or consolidated approach may need to be adopted, too cumbersome;
- Establish a reasonable and usable set of profiles;
- Some discussion on why SP 800-53 Moderate Impact control baseline used; too restrictive, should have more granular levels of "classification";
- App vetting is necessary but not sufficient - have to monitor app behavior and context of usage;
- Good policy, guidance and infrastructure (PIV-1, PIV, CAC). Problem with how it is being implemented differently by branch/agency (e.g., DOD approach defined but not being implemented consistently);
- Improve the use of credentials (e.g., PKI, PKE) stored in hardware root of trust (e.g., TPM);
- Continue to move to biometrics or other multi-factor options;
- The Federal Government does not have a standard mobile application development process for industry to follow. The concept of developing a "FedRAMP for Mobile" was a recurring theme; and
- Need to address the entire mobile application lifecycle not just MAS and MAM.

Acknowledgments

This document is the product of a multi-agency collaboration to provide guidance for the successful implementation of moderate level baseline for mobile device implementations for Federal civilian departments and agencies. Participants from several departments and agencies have graciously volunteered their expertise; this document would not be possible without their selfless contributions. Individuals from departments and agencies that contributed to the development of the mobile computing security baseline are as listed below.

Mobile Computing Security Baseline Team

Name	Organization
Roger Seeholzer	Department of Homeland Security- Lead
Greg Youst	Department of Defense/Defense Information Systems Agency
Kevin Cox	Department of Justice
Kelley Dempsey	National Institute of Standards and Technology
Josh Franklin	National Institute of Standards and Technology

Special Acknowledgements

Name	Organization
David Carroll	Department of Homeland Security - Mobile Technology Tiger Team Co-Chair
Kevin Cox	Department of Justice - Mobile Technology Tiger Team Co-Chair
Raj Pillai	General Services Administration - Mobile Technology Tiger Team Co-Chair
Chi Hickey	General Services Administration - Mobile Technology Tiger Team Co-Chair
Mark Norton	Department of Defense
Vincent Sritapan	Department of Homeland Security
Kris Lee	Department of Homeland Security
Harry Clarke	National Security Administration
Adam Sedgewick	National Institute of Standards and Technology
Debra Danisek	Department of Homeland Security
Robert Palmer	Department of Homeland Security
Phil Loranger	Department of Defense
Marilyn Rose	Department of Homeland Security